INFORMATION OPERATIONS
&
SECURITY

Integrity ★ Service ★ Excellence

5 MAR 2012

DR. ROBERT HERKLOTZ
PROGRAM MANAGER
AFOSR/RSL
Air Force Research Laboratory

DISTRIBUTION A: Approved for public release; distribution is unlimited.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **05 MAR 2012**	2. REPORT TYPE	3. DATES COVERED **00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE **Information Operations & Security**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Laboratory,Wright-Patterson AFB,OH,45433**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Presented at the Air Force Office of Scientific Research (AFOSR) Spring Review Arlington, VA 5 through 9 March, 2012

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**40**	

2012 AFOSR SPRING REVIEW

NAME: DR. ROBERT HERKLOTZ

BRIEF DESCRIPTION OF PORTFOLIO:
Fund science that will enable the AF and DOD to dominate cyberspace: Science to develop secure information systems for our warfighters and to deny the enemy such systems.

LIST SUB-AREAS IN PORTFOLIO:
1: SOS-Science of Security
2: Secure Humans
3: Secure Networks
4: Secure Hardware
5: Covert Channels
6: Execute on Insecure Systems
7: Secure Data
8: Secure Systems-Security Policy

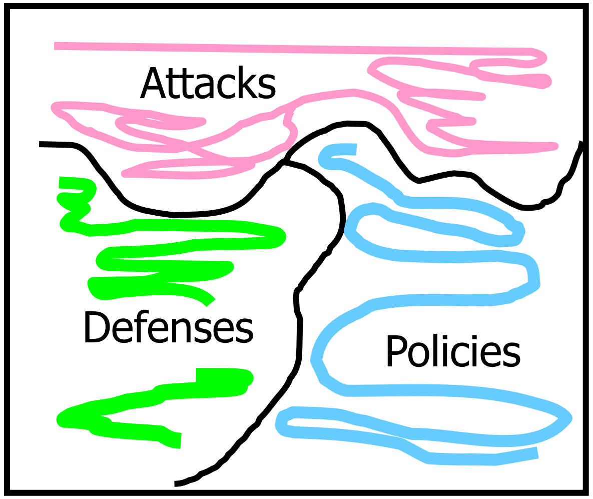
Information Operations and Security 61102F

Cyber Security

MOTIVATION

- Cyber Security basic research has the potential to change the current balance that favors the attackers
- Discovery and development of a Science of Cyber Security (SOS) should be vigorously pursued
- Develop methods to execute mission while under attack

PICTURE



TECHNICAL IDEAS

- Science of Security: formally model relationships between attacks, defenses and policies and invent good metrics
- Develop a theory of Covert Channels
- Pursue methods to execute mission on insecure components

PAYOFF

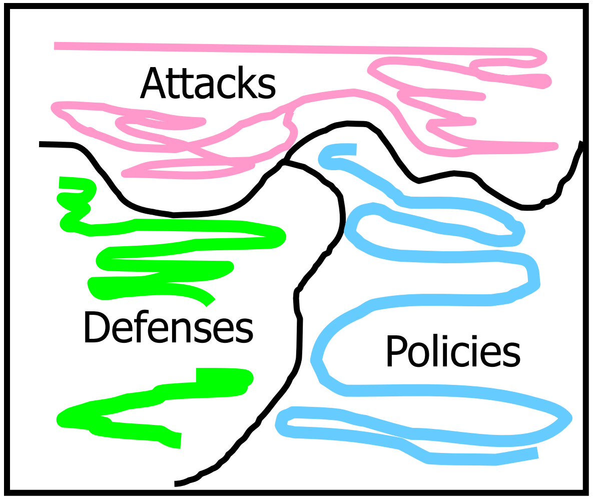
- Inherently secure software and hardware systems can be deployed in the future
- Covert channels can be anticipated and denied or used
- Insecure, distributed systems can be used to execute the mission

Level 3

SOS Laws: Analysis and Synthesis

- Science:
  - Laws or theories that are predictive
- Analysis: Given an artifact, predict its properties…
  - Qualitative properties: What it does?
  - Quantiative properties: How well?
- Synthesis: Compose artifacts with given properties to obtain a new one with predictable properties.

SOS: Laws about What?



- **Features:**
  - **Classes of policies**
  - **Classes of attacks**
  - **Classes of defenses**
- **Relationships (= SoS)**
  - **Defense class D enforces policy class P despite attacks from class A.**

AFOSR MURI Project

Sept 23, 2011

Science of Cyber Security: Modeling, Composition, and Measurement

Anupam Datta (CMU)
Joe Halpern (Cornell)
John Mitchell (Stanford, PI)
Andrew Myers (Cornell)
Andre Scedrov (U Penn)
Fred Schneider (Cornell)
David Wagner (UC Berkeley)
Jeannette Wing (CMU)
Ittai Abraham (Microsoft Research, unfunded collaborator)

Stanford, Berkeley, Carnegie-Mellon, Cornell, U Penn

SOS MURI Goals

- Scientific objective
  - Advance the science base for trustworthiness by developing concepts, relationships, and laws with predictive value.
- Technical approach
  - *Security modeling:* characterize system, threats, and desired properties. Leverage game-theoretic concepts to model incentives for the defender and attacker.
  - *Composition:* develop principles for explaining when security schemes compose, and how to achieve compositionality.
  - *Security Measurement:* goals include determining relative strengths of defense mechanisms, evaluating design improvements, and calculating whether additional mechanism is warranted based on attacker and defender incentives

Science Base for Evaluation and Characterization of System Trustworthiness-SOS Metrics

Fred B. Schneider
Department of Computer Science
Cornell University
Ithaca, New York

DISTRIBUTION A: Approved for public release; distribution is unlimited.

Kinds of Analysis Laws

- **Analysis: Given an artifact, predict its properties…**
  - **Qualitative properties: What it does.**
  - **Quantitative properties: How well it works.**
- **Synthesis: Compose artifacts with given properties to obtain a new one with predictable properties.**

The Promise of Security Metrics

- **Users: Purchasing decisions**
  - **Which system is the better value?**
- **Builders: Engineering trade-offs**
  - **Select among different designs?**
- **Researchers: Evaluating new ideas**
  - **Basis for declaring success!**

Definition: Security Metric

“μ is a security metric” should mean…

- **μ: Systems → Vals, where:**
  - < is a partial order on Vals

    … so theory applies to more “metrics”. E.g.,

    μ(S) = {all attacks that compromise S}
  - μ(S) is efficiently computable
  - x<y is efficiently computable

Intent: < reflects “actual security”, so

μ(S)< μ(S’) means S is less secure than S’

Properties of Security Metrics

Define: S«S’ – S is “less secure than” S’

Soundness of µ: (Useful for users)

µ(S)< µ(S’) implies S«S’

Completeness of µ: (Useful for engineers)

S«S’ implies µ(S)< µ(S’)

S«S’: The Fine Print

If S«S’ holds then …

S, S’ must implement “same” specification:

- **Specification defines an interface.**
  - **All** interactions with the system involve actions in this interface. E.g., Includes side-channels.
- **Specification describes expected effects of actions at the interface.**

An attack is an input that causes the specification to be violated.

The $64,000 Question!

For what classes of specifications do there exist sound (and complete?) security metrics?

Conjecture:

- Expressive specs IMPLY security metric μ must be undecidable or μ incomplete.
- Security metric μ decidable and soundness IMPLY F expressiveness is bounded by static type checking.

Non-Intrusive Media Forensics Framework

K. J. Ray Liu and Min Wu

Department of Electrical and Computer Engineering

University of Maryland, College Park

DISTRIBUTION A: Approved for public release; distribution is unlimited.

Digital Multimedia Anti-Forensics

- Very little consideration has been given to *anti-forensic operations*
  - Designed to remove/falsify intrinsic fingerprints
  - Create undetectable forgeries

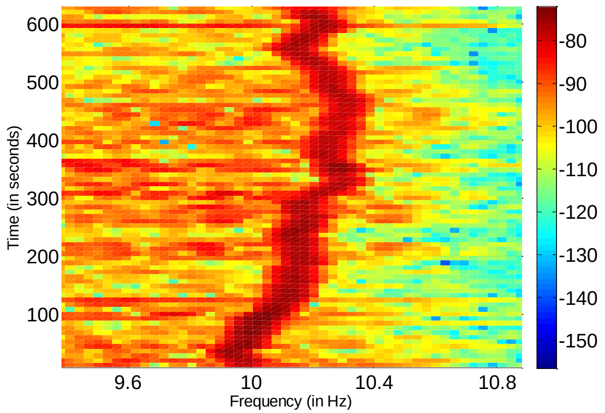
- *The study of anti-forensics is*
  - Identifies weaknesses in existing forensic techniques
  - Important for the development of tools to detect the use of anti-forensic operations

ENF: A Ubiquitous and Natural Fingerprint

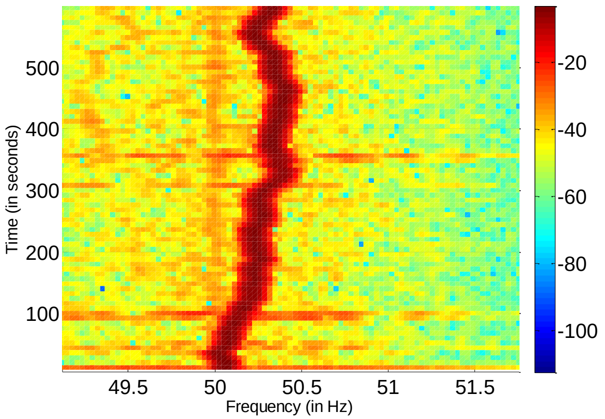
- **ENF: Electrical Network Frequency**
  - **60 Hz in North America, 50 Hz elsewhere (50/60 Hz in Japan)**
  - **Electro-magnetic (EM) field from power grid interferes with electronic recording mechanisms (Sensors)**
- **ENF varies slightly from 50/ 60 Hz over time**
  - **Deviations depends on regulations: ~ on the order of 0.05-0.1Hz**
  - **Main trends are the same over the power grid [1]**
- **ENF can be "heard" and "seen"**
  - **Present in audio recordings near power sources**
  - **We showed luminance of indoor lightings fluctuates based on ENF**
    - Captured by optical sensors: photo diode, CCD camera sensors, etc.
  - **Random deviations can be used as fingerprints for multimedia content:**
    - Determine the time and place of recordings
    - Detect tampering in the multimedia content; bind video and audio

[1] C. Grigoras. Applications of ENF criterion in forensics: Audio, video, computer and telecommunication analysis. *Forensic Science International*, 167(2-3):136 – 145, April 2007.

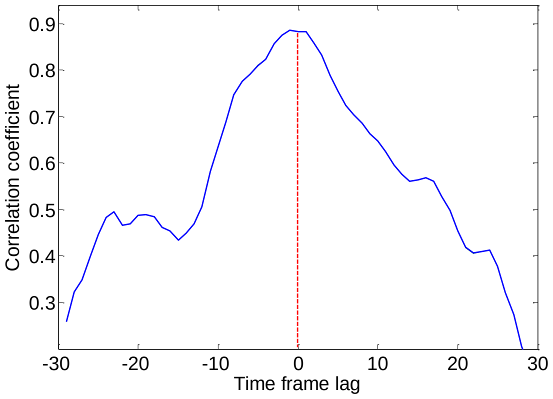
Verify Time of Recording



Video ENF signal



Power ENF signal



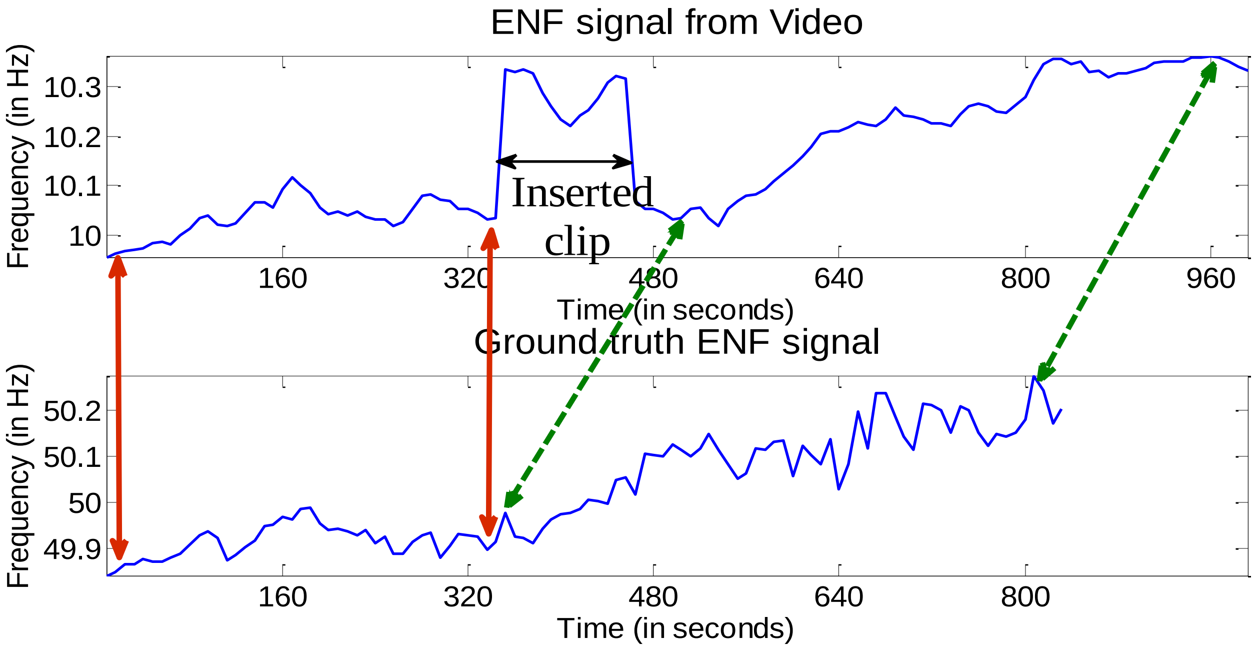
Normalized correlation

ENF matching result demonstrating similar variations in the ENF signal extracted from video and from power signal recorded in India

- Aliasing Challenge with video: temporal sampling rate lower than ENF
- Our recent results from US, China, and India power grids
  - Exploit signal processing to harvest from aliasing
  - **Highest correlation between power ENF and video ENF signal corresponds to the time at which recording took place**

Tampering Detection

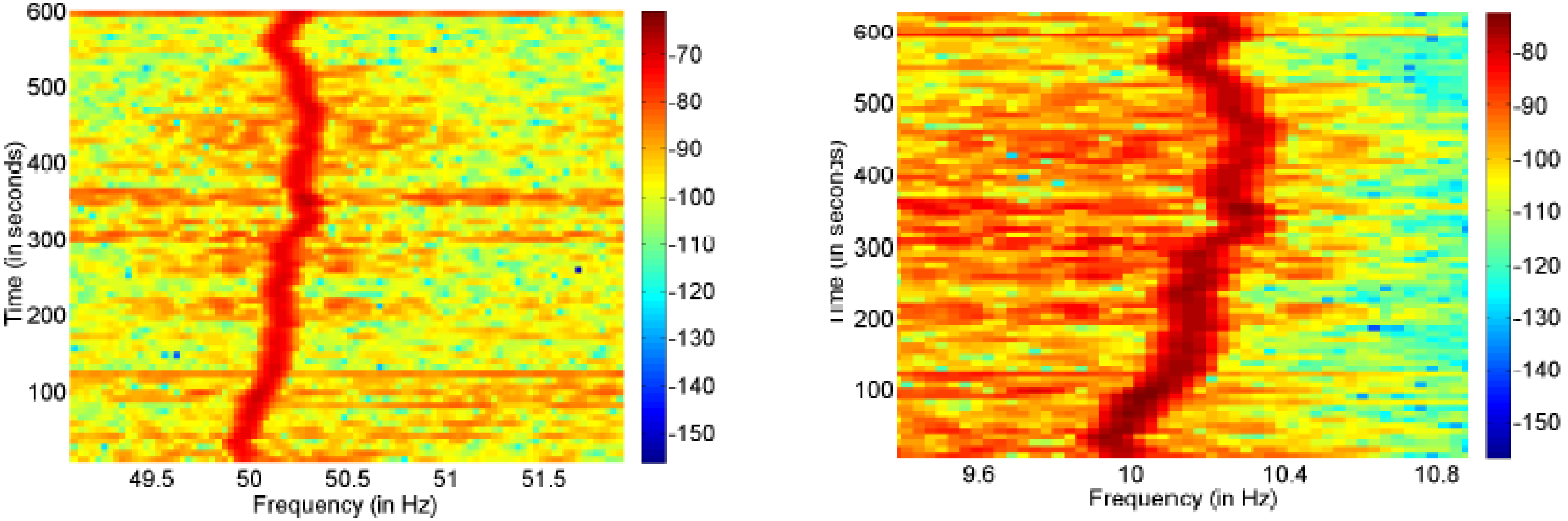
ENF matching result demonstrating the detection of video tampering based on the ENF traces



- **Adding a clip between the original video leads to discontinuity in the ENF signal extracted from video**
- **Clip insertion can also be detected by comparing the video ENF signal with the power ENF signal at corresponding time**

Forensic Binding of Audio and Visual Tracks

- **ENFs in audio and video tracks captured at the same time have high correlation**



(a) ENF signal from the audio track

(b) ENF signal from the video track

- **Research questions ahead:**

  (1) How to accurately estimate and match weak and noisy ENF? (2) Can ENF be removed? Tampered? (3) How to prevent anti-foreniscs on ENF? ……

AFOSR INFORMATION OPERATIONS & SECURITY 2011 PI MEETING
19-23 SEPTEMBER 2011
ALINGTON, VA

AFRL
THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER

High Performance Semantic Cloud Auditing

CyberBAT

Keesook J. Han, Ph.D

Keesook.Han@rl.af.mil

Develop High Performance Semantic Cloud Auditing Technologies and Applications that includes Comprehensive Cloud Auditing Data Capturing, Analysis and Rapid Response to Improve Cloud Quality of Services.

Approved for Public Release; Distribution Unlimited: 88ABW-2011-4496, 16-Aug 2011

Cloud Research Facilities

University of Texas at San Antonio
FlexFarm (Honeyfarm)&FlexCloud: Institute for Cyber Security

Texas A&M University
Cisco Test Engineering Center
Cisco Cloud Testing Lab

University of South Carolina
Router Testbed: Center for Information Assurance Engineering

University of Texas at Dallas
UTD Secure Cloud Repository: Hadoop File System

SUNY Binghamton University
GPGPU Cluster: Real-Time Embedded Systems Lab

University of Illinois at Urbana Champaign
Coordinated Science Lab Assured Assured Cloud Computing Center

Tennessee State University
Center of Excellence in Information Systems and Engineering Management

Rochester Institute of Technology
Networking, Security, and Systems Administration Labs

University of Pittsburgh
Swanson Institute for Technical Excellence

University of Missouri Kansas City
Networking & Multimedia System Lab

AFRL RI
GPGPU Cluster: CONDOR Supercomputer

Georgia Institute of Technology
Foundations of Data and Visual Analytics Center

Conclusion

➢ Semantic Cloud Auditing:

Develop Efficient Information Theoretic Metadata and Aggregation: Fast Information Exploitation of Massive Cloud Auditing Data for Rapid Response

➢ Semantic Cloud Auditing will benefit to the following projects:

- **Access Control:** "Advanced Access Control for Assured Clouds"
- **Cloud Security:** "Honeyfarm Data Capturing, Rapid Sharing and Exploitation of Malicious Traffic for Cloud Security"
- **Customized Hadoop:** "Massive Cloud Auditing Using Data Mining on Hadoop"
- **Secure Hadoop:** "Assured Information Storage and Sharing on Hadoop"
- **GPGPU Computing:** "High Performance Processing of Cloud Auditing Data Using GPGPU Many-Core Parallelism"
- **SLA-based Cloud Service Workloads:** "Dynamic Mapping of Cloud Resources to Meet Service Level Agreement (SLA)-based Cloud Service Workloads"
- **Traffic Control:** "Router-Based Filtering and Rerouting to Traffic Control in Cloud Computing"
- **Outage Management:** "Router-Initiated Network Outage Management for Multitenant Clouds"
- **File Transfer:** "Bandwidth Intensive Multimedia Data Transfer for Smartphone-Friendly Cloud Services"

POC: AFRL/RIGA Dr. Keesook.Han@rl.af.mil

Detection of Covertly Embedded Hardware in Digital Systems

Douglas H. Summerville

Associate Professor

Electrical and Computer Engineering

State University of New York at Binghamton

DISTRIBUTION A: Approved for public release; distribution is unlimited.

Covertly Embedded Trojan

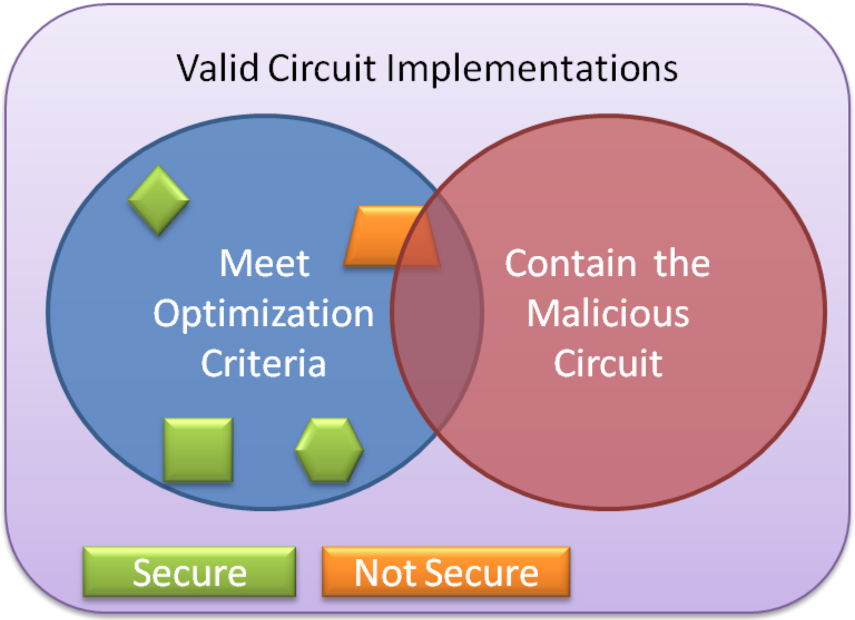
- **Malicious circuit embedded in "implementation space" of its host**
  - **Neither functional nor parametric**
- **Trojan uses *existing resources* that are artifacts of the host's implementation**
- **No alteration of functional characteristics of host, therefore not testable**
- **Can be combinational or sequential circuits**

The Embedding

- Covert Hardware alters the circuit’s behavior in the “don’t care” space
- In effect, two circuits co-exist in the same physical hardware
  - The original circuit, only exercised during normal operation
  - The malicious circuit, exercised by special trigger

Motivating Assumption

- **Assume general case is unsolvable**
- **In practice, standard design approaches generate a small fraction of possible implementations**
- **We focus on securing few practical cases**


Valid Circuit Implementations
Meet Optimization Criteria
Contain the Malicious Circuit
Secure
Not Secure

Structural Circuit Analysis

- Can’t look at circuit’s function, so look at its structure
- Exploits how design approaches optimize for speed, area, power, etc. in deterministic ways
  - Contributing regularity to circuit structure
- Identify structural characteristics of circuits that
  - Result from standard design approaches
  - Are removed or altered by tampering
- Restrict optimization to solutions in that space
  - tradeoff

Detecting Hidden Communications Protocols

R. R. Brooks
Associate Professor
Holcombe Department of Electrical and Computer Engineering
Clemson University
Clemson, SC 29634-0915
Tel. 864-656-0920
Fax. 864-656-1347
email: rrb@acm.org

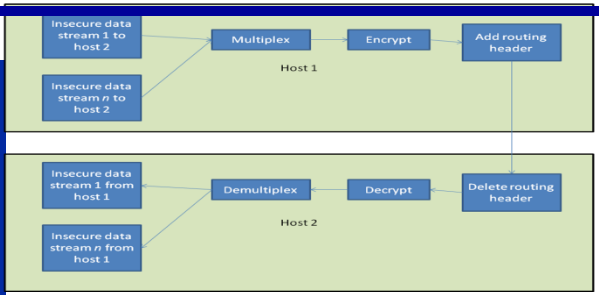
Detection of Hidden Communications Protocols

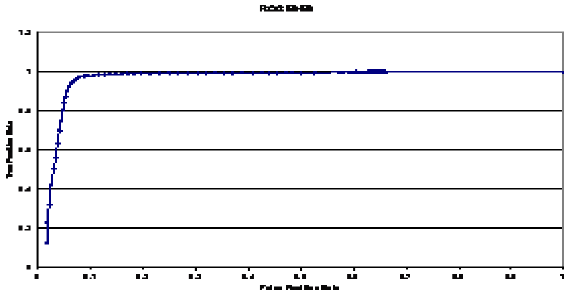
Richard Brooks: rrb@acm.org, Clemson University

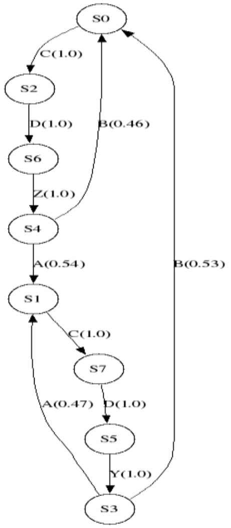
Objective

Detect use of tunneled communications protocols and infer their current internal state

- Private communications often tunneled through virtual private networks (VPNs)
- Mix networks tunnel connections for anonymity
- Tunneling tools (ex. ssh, ssl, TOR) have timing vulnerabilities
- Hidden Markov models (HMM) and probabilistic grammars will detect protocol use, infer network flows, partially decipher content


Insecure data stream 1 to host 2
Insecure data stream *n* to host 2
Multiplex
Encrypt
Add routing header
Host 1
Insecure data stream 1 from host 1
Insecure data stream *n* from host 1
Demultiplex
Decrypt
Delete routing header
Host 2





DoD Benefit:

- Detection of tunneled communications protocols
- In some cases (ex. interactive ssh), partially decipher message contents
- Determination of communications patterns in mix networks, such as TOR
- Detection of timing side channel attack vulnerabilities in DoD networks

Technical Approach:

- Collect inter-packet timing information from tunneled sessions
- Zero-knowledge HMM model inference
- Determination of HMM statistical significance
- Tracking HMM transitions driven by network flow inter-packet timing data detects protocol use
- Viterbi algorithm finds maximum likelihood Markov state sequence
- Two point-to-point connections with same Markov state sequences (Viterbi paths) are likely data source and sink

Active Defense: Reactively Adaptive Malware: Attacks & Defenses

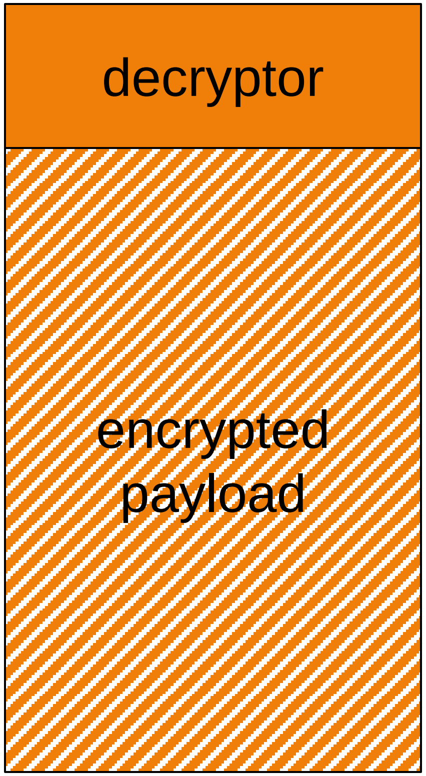
Kevin W. Hamlen & Latifur Khan
University of Texas at Dallas

AFOSR Contract FA9550-10-1-0088

September 2011

Attacks Upon Signature-matchers

- **Randomize features during propagation**
  - **Polymorphism**
    - encrypt payload with randomly chosen key
  - **Oligomorphism**
    - randomly re-assemble decryptor
  - **Metamorphism**
    - non-deterministically recompile decryptor and/or payload
- **Weakness: <u>Undirected</u> mutation**



Reactively Adaptive MALware (RAMAL)

- **Three challenges:**
  1. **Covertly harvest data about victim defenses (malware signature databases)**
  2. **Mine harvested data effectively**
  3. **Derive new mutation strategy from inferred model**

Hardware, Languages, & Architectures for Defense Against Hostile Operating Systems (DHOSA)

V. Adve, UIUC

K.Asanović, UC Berkeley

D.Evans, UVA

S.King, UIUC

G.Morrisett, Harvard

R.Sekar, U Stony Brook

D.Song, UC Berkeley

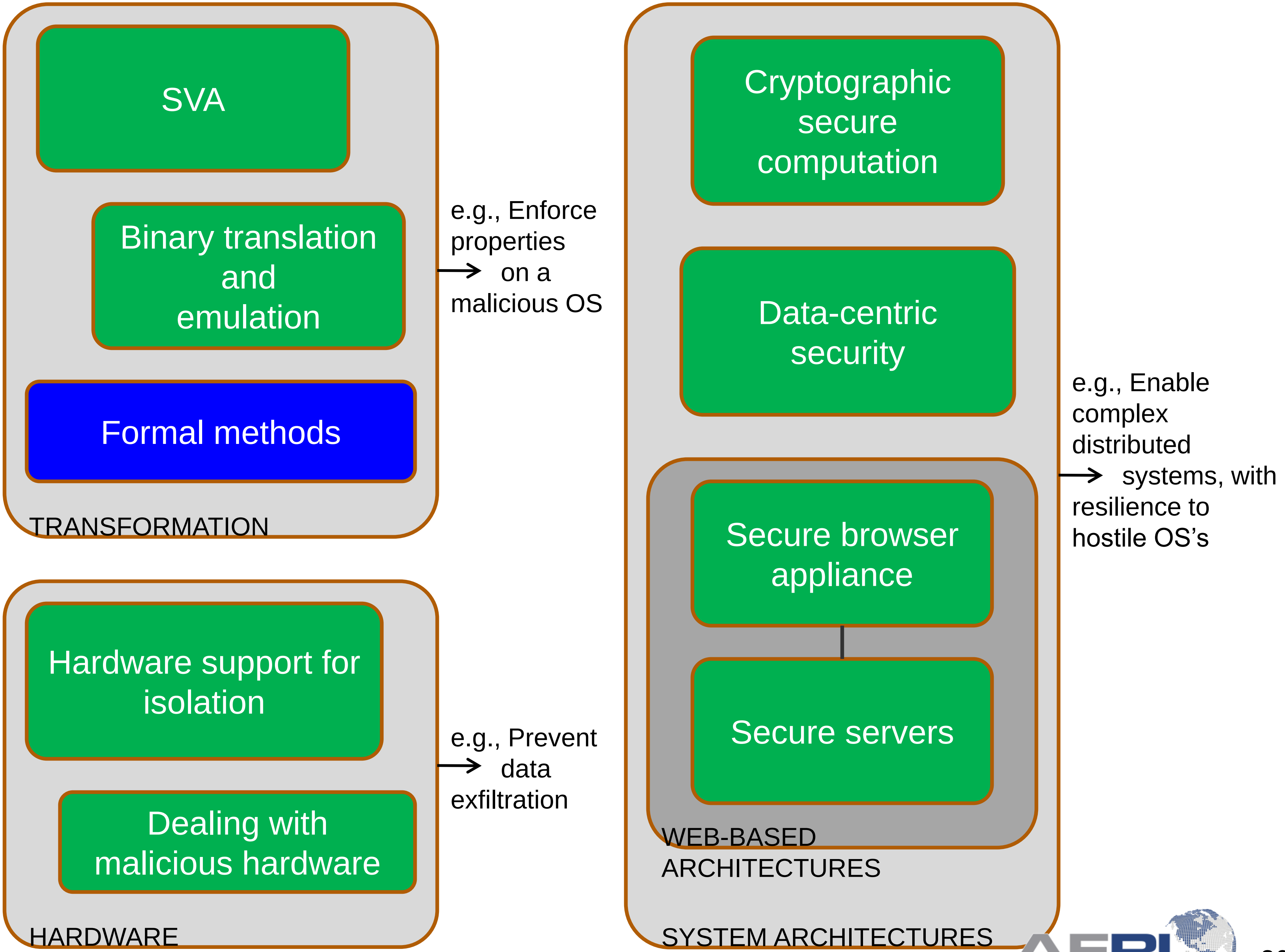
D.Wagner (PI), UC Berkeley

http://www.dhosa.org/

The Approaches

Advances that cut across traditional disciplines:

- **new OS and software architectures**
- **new hardware architectures**
- **new policy enforcement techniques**
- **new techniques for trustworthiness**
- **new coding techniques**



SVA

Binary translation and emulation

Formal methods

TRANSFORMATION

e.g., Enforce properties → on a malicious OS

Hardware support for isolation

Dealing with malicious hardware

HARDWARE

e.g., Prevent → data exfiltration

Cryptographic secure computation

Data-centric security

Secure browser appliance

Secure servers

WEB-BASED ARCHITECTURES

SYSTEM ARCHITECTURES

e.g., Enable complex distributed → systems, with resilience to hostile OS's

Helix:

A Self-Regenerative Architecture for the Incorruptible Enterprise MURI 2007 - 2012

John Knight

University of Virginia

AFOSR PI Meeting
9/21/2011

Helix Team Members

- University of Virginia
  - John C. Knight (PI) - Software engineering, dependability
  - Jack W. Davidson - Languages, security, virtual machine
  - David Evans - Security, applied cryptography
  - Westley Weimer - Program analysis
  - Anh Nguyen-Tuong - Security, grid computing
- University of New Mexico
  - Stephanie Forrest - Biological inspired computing
  - Jared Saia - Computational & game theory
- University of California at Davis
  - Hao Chen - Security, Web applications
  - Zhendong Su - Program analysis, software engineering
  - S. Felix Wu - System fault tolerance
  - Jeff Rowe - Operating systems
  - Karl Levitt - Security
- University of California at Santa Barbara
  - Frederic Chong - Secure hardware, hardware acceleration for program/system analysis

Research Highlights

- **Security for mobile devices:**
  - **Static analysis framework for detecting information leaks (Android)**
- **Security for web applications:**
  - **Static analysis to detect access control vulnerabilities**
- **Security for applications:**
  - **Detection of unsafe component loading**

- **Automated repairs via genetic programming:**
  - **Demonstrated on assembly code**
  - **Proactive diversity/variant generation**
- **Hardware/architecture for security:**
  - **Hardware description language (compiler released)**
  - **Provably leak-free hardware**

See web site: http://helix.cs.virginia.edu

9/21/2011

DISTRIBUTION A: Approved for public release; distribution is unlimited.